What Every Campaign Staffer Should Know About Cybersecurity

Congratulations, you're a cyber target.

Whether you're an intern or the campaign manager, cyber criminals are trying to break into your accounts and steal the campaign's information. Everyone has a responsibility to protect themselves and the campaign. That includes you.

There are simple things you ***must*** do to avoid making yourself and the campaign a victim.

1. Activate Two-Factor Authentication

Adding two-factor authentication to your email, file storage, and social media accounts is the most important step you can take to secure your information and it's really simple to set up. Your campaign will tell you which two-factor method to use. Two-factor authentication makes it a lot harder for the bad guys to get into your account, even if they steal your password.

2. Create Strong Passwords

Make your password as long as possible. Think of it more as a "pass-sentence" than a password. Less than 8 characters is too short. 12 or longer is much better. Contrary to popular belief, it should not include requirements for numbers, special characters, or capitalization. `SOMETHINGLIKETHISPASSWORDHERE` is actually harder to hack than `s0m3TH!n6L1k$`. String a set of words together that are easy for you to remember. Don't write your password down where someone can find it. If you have even a faint suspicion that someone might know your password, change it immediately.

3. Keep work on your work accounts

Never use your personal email or storage services for campaign work. Foreign agents have hacked people's personal email accounts in the past to steal information. To keep your personal life secure, use strong passwords and two-factor authentication.

(Continued on back)

4. Secure your personal accounts

Make sure you have two-factor and strong passwords on your personal accounts, just in case someone tries to hack your personal life. If you are on Gmail, there's a service for personal accounts called Advanced Protection that uses physical keys to give you extra protection from someone else logging onto your accounts. There is also a Chrome extension you can download that helps protect Gmail accounts against phishing.

5. Watch out...

a. **Clicking links.** Avoid clicking links in emails; go directly to a site through your browser instead. Just clicking a malicious link can install malware on your computer. Be especially careful of links that ask for your password or personal information. If you see something suspicious, contact us immediately!

b. **Trust your gut.** If an email looks funny or has strange grammar, don't click anything or open any attachments. If a co-worker seems to be sending a strange request, or asking you to share something sensitive over email, pick up the phone and call them to make sure it's legit. Never click links, open attachments, or send sensitive information in response to emails from people you don't know or addresses you don't recognize. If you see something suspicious or aren't sure what to do, just say so!

c. **Downloading apps.** Only download apps from the official Apple or Android store on your device. Avoid downloading apps you don't need, since adversaries will sometimes spy on your computer or phone by creating apps disguised as games or helpful tools.

d. **Social media**. Your social media accounts contain a wealth of information about you and your whereabouts that hackers can use to send you sophisticated phishing emails. Limit the information you share by default and select security settings that allow only accepted friends to see personal information. Don't accept friend requests from people you don't know.